# 電子証明書をとりまく動向


2017年6月9日 学術情報基盤オープンフォーラム

国立情報学研究所 水元 明法

# テーマ

- UPKI電子証明書発行サービス最近のアップデート
- これからの動き
- 事件簿

# S/MIME専用認証局の追加

- クライアント証明書とS/MIME証明書の発行認証局を分離しました
  - NII OpenDomain CA - G4 （既存）
  - NII Open Domain S/MIME CA （新設：S/MIME専用）
- Microsoft Root Programの変更によるものです
  - サーバ証明書、コード署名用証明書、S/MIMEの各用途の証明書は、それぞれ別のCAから発行すること
  - http://social.technet.microsoft.com/wiki/contents/articles/31633.microsoft-trusted-root-program-requirements.aspx
- 発行済みのクライアント証明書（S/MIME含む）の失効は不要です。これまで通りご利用いただけます。
- ルートCAに、追加・変更はありません。
- 発行申請用TSVのフォーマットにも変更はありません。

# コード署名用証明書の仕様変更1

- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificatesへの対応
  - 証明書の主体者DNに「L=市区町村」「S=都道府県」が設定されます
    - 申請用TSVには旧来通り S= 使用しない L=Academe を記載
    - 証明書発行時に、サービスに登録済みの住所をもとに両者を設定
    - この処理のため、発行に１～２営業日を要します
  - コード署名用証明書のダウンロード方式はCSR発行のみとします
    - P12でのダウンロードを廃止します
    - 秘密鍵管理を厳格化するためです
    - コード署名用証明書の厳格な管理をお願い申し上げます
      - USBメモリ等の外部媒体へ保存し鍵付きキャビネット等に保管
      - アクセス権限制限を設けた任意のフォルダにて厳重に管理
        など

# コード署名用証明書の仕様変更2

- Minimum Requirements対応（続き）
  - OCSPへの対応
    - OCSPサーバによるステータス情報の提供を開始します
      - CRLによるものも引き続きご利用いただけます
    - これまで発行されたコード署名用証明書の失効は不要ですが、OCSPに対応した証明書が必要な場合は、新規もしくは更新で取得してください。
  - タイムスタンプの試験提供（限定提供）
    - メールもしくはその他の手段で、サービス窓口宛にコード・アプリケーション等を送付の上、ご依頼ください
      - 手動対応のため、処理に数日頂戴します

# 登録担当者用証明書の更新について

- 2017年1月で、サービス開始から2年が経過します
- 登録担当者用証明書は25ヶ月(2ヶ年+30日)で有効期限満了となります
- 2017年早々に更新作業が必要になります
  - 例:
    - 2015年1月に登録担当者用証明書取得
      →有効期限は2017年2月
  - 有効期限の30日前から、更新申請が可能になります
  - 証明書の更新には、申請と本人確認が必要です
  - 旧プロジェクトでは電話での連絡が必要でしたが、本サービスではUPKI申請システムを用いて更新申請できるようにいたします

# UPKI申請システム

- これまでExcelファイルで作成いただいていた各申請書が、Webサービスで作成できるようになりました
- https://certs-office.nii.ac.jp
- UPKIに関する全ての申請書が作成できます
  - ドメイン申請
  - 機関情報変更申請
  - 登録担当者情報変更申請
  - 利用期間更新申請
  - サービス利用申請
  - 確認実施手順調査票 提出・変更
  - 体制図 提出・変更
  - 登録担当者用証明書更新申請 New!
- 各申請に、登録担当者と窓口担当者がコメントをつける形で、修正点などやりとりできます

# DNS-CAAのチェックが必須になります

- 2017年9月8日以降にSSL/TLSサーバ証明書を発行する際、認証局に、DNS CAA（Certification Authority Authorization）レコードの検証が義務づけられることになった
  - DNS CAAレコード(RFC6844)
    - 信頼する認証局を記述できるレコード
    - 認証局は証明書発行時にこのレコードを参照する
    - ここに記述のない認証局での発行要求があった場合、証明書を発行せず、レコード記載のメールアドレスもしくはURLに通報する
- CA/ブラウザフォーラムによる the Baseline Requirements 変更によるもの
  - 認証局の義務であって、ドメインを管理する者に記述が義務づけられるものではない

# ChromeのCT対応が必須になります

- CT:Certificate Transparency
  - 証明書発行の透明性
  - 共通の基準により、ログに記載する
- 当初はEVのみであったものが、OV(UPKIの証明書はこちらです)、DVにも適用されることとなった
- 2017年10月から、とされていましたが、これが来年に延期になっています
- 来年からのUPKI電子証明書発行サービスでどうするのか？は、次の発表で

# Let's EncryptとComodoのTLS証明書、96%の詐欺サイトで使用

- Let’s Encrypt and Comodo issue thousands of certificates for phishing
  - https://news.netcraft.com/archives/2017/04/12/lets-encrypt-and-comodo-issue-thousands-of-certificates-for-phishing.html
- フィッシングサイトの96%は、両認証局によって証明書が発行されている
- 自動化され、費用もかからない点が魅力か？
- 当該サイトが正規のものかどうかの判断基準
  - 依然として残るOV、EVの強み
  - ただしChromeでは・・・

# StartCOMとWoSign

- 2016年9月～10月 Apple, Google, Mozilla はWoSignとStartComが発行した証明書について、それぞれが設定した日時以降に発行した証明書を信用しない、とした
  - https://security.googleblog.com/2016/10/distrusting-wosign-and-startcom.html
  - https://blog.mozilla.org/security/2016/10/24/distrusting-new-wosign-and-startcom-certificates/
  - https://support.apple.com/en-us/HT204132
- 「SHA1で署名された証明書は2016年1月1日以降発行しないこと」としていた業界団体の定めに反し、発行日を偽装した証明書を発行していたことが明らかになったため。
  - これを含め、証明書発行のプロセスにも問題がみられたとしている

# Symantec(1)

- Symantec傘下のThawte（ソート）による、google.com および www.google.com 用EV証明書不正発行事件（2015年9月14日）
- Improved Digital Certificate Security
  - Google Security Blog
    - https://security.googleblog.com/2015/09/improved-digital-certificate-security.html
  - ドメイン持ち主のGoogleへの確認をとらずに発行
  - Googleは、CT（証明書発行の透明性）ログから見つかったとしている

# Symantec (2)

- 2017年3月24日
  - Symantecが、自身が所有しないドメインに対して、テスト証明書を発行していることがCTログから見つかった
    - 前項の事件の後、再発防止策がSymantec側から提示されていたが、これが全く徹底されていない としている
  - これをうけて、Googleのエンジニアは下記2点の提案を行う
    - 米Symantecと傘下の認証局から新規に発行されるSSL/TLS証明書について、有効期限を段階的に短縮し、Chrome 64で279日以内の証明書しか受け入れないようにする
    - またアドレスバーのEV表示（緑色の機関名表示）を停止する
      - https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ
- Symantecも当然反論しているが・・
  - https://www.symantec.com/connect/ja/blogs/symantec-backs-its-ca-0

# Symantec (3)

- 前項の記事が公表されるのと時期を同じくして、SymantecのEV証明書が、Chromeのアドレスバーにおいて通常のOVやDV証明書と同様の表示になった。
  - http://forest.watch.impress.co.jp/docs/news/1051745.html
- Chrome57のバグであり、Chrome58にて修正
  - https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=INFO4287

# まとめにかえて

- 制度的な変更が継続してみられます
  - 本サービスでは、可能な限りそれらをフォローできるよう努めて参ります
- 電子証明書発行に関するいくつかのニュースをとりあげてお伝えしました
  - 本サービスでは、サービス利用機関に、証明書発行時の確認作業を実施いただいています
    - サービス利用申請・ドメイン申請時にいただいた「確認実施手順調査票」によるものです
    - こちらに準拠して証明書発行時の確認を実施していただければ、そうそう事故が起こるものではありません
- UPKI電子証明書発行サービスの維持のため、引き続きのご協力をお願い申し上げます

# EV証明書について

- 本サービス利用機関(※)に対し，証明書発行もとであるセコムトラストシステムズより，EV証明書が有償で提供されます


※サービスに登録したドメインである必要はありません

- ご希望の機関には，セコムトラストシステムズより提供された「申請ガイド」を送付いたします
  - certs@nii.ac.jp までご依頼ください！
  - 「申請ガイド」受領以降のEV証明書についてのお問い合わせ，発行手続き，お支払い等は，セコムトラストシステムズと直接行ってください

# EV SSL証明書(セコムパスポートforWeb EV2.0) の特徴

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

## ◆ 機能　　アドレスバーが緑色に変化し、安全性をアピール

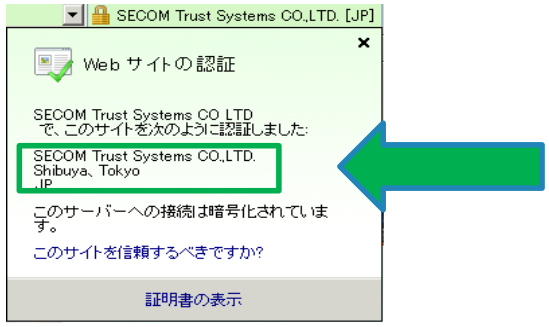

**EV SSL証明書対応ブラウザでアクセスすると、アドレスバーが緑色に変化**

OV(組織認証)証明書(セコムパスポートforWeb SR3.0)では、https://でアクセスしてもアドレスバーの色は白色のままです。


**危険なサイトはアドレスバーが赤色に変化**

https://でアクセスしたとき、「失効されている」「有効期限が切れている」「Webサイトの URLと一致していない」疑わしいサイトの場合には、危険なサイトとして、アドレスバーが赤色に変化します。

## ◆ 効果　　識別情報の表示で運営組織を確認、 フィッシング対策に有効




従来、ブラウザの鍵マークをクリックしなければ確認できなかった「**サーバー証明書に記載されている組織名**」がアドレスバーの横に表示されます。

EV SSL証明書は、実在証明としてより一層安全性をアピールすることができます。

Secured by SECOM

セコムのWebステッカーがEV SSL証明書の更なる安全性を訴求